

WHAT IS CLAIMED IS:

Sub  
AB  
1. A system comprising:  
2 a communications engine for establishing a communications  
3 link with a client;  
4 security means coupled to the communications engine for  
5 determining client privileges;  
6 a servlet host engine coupled to the security means for  
7 providing to the client, based on the client privileges, an applet  
8 which enables I/O with a secured service; and  
9 a key safe for storing a key which enables access to the secured  
10 service.

500  
26040 05674330  
H2  
1. The system of claim 1, wherein the communications engine  
2 uses SSL technology to create a secure communications link with the  
3 client.

1. The system of claim 1, wherein communications engine  
2 negotiates an encryption protocol for transferring messages to and  
3 from the client.

1 4. The system of claim 1, wherein the communications engine  
2 uses public key certificates for transferring messages to and from the  
3 client.

1 5. The system of claim 1, wherein the security means uses public  
2 key certificates to authenticate the client.

1 6. The system of claim 1, wherein the security means examines  
2 client identity and the level of authentication to determine client  
3 privileges.

1 7. The system of claim 1, wherein the security means examines a  
2 global certificate to authenticate the client.

1 8. The system of claim 1, wherein the security means uses digital  
2 signature technology to authenticate the client.

1 9. The system of claim 1, wherein the servlet host engine  
2 forwards to the client a security applet for enabling the client to  
3 perform a security protocol recognized by the security means.

268040 056T4880

1 10. The system of claim 1, wherein the service is secured by a  
2 corporate firewall and the key is configured to enable communication  
3 through the firewall.

1 11. The system of claim 1, further comprising a global firewall for  
2 protecting the system.

1 12. The system of claim 1, further comprising a service address for  
2 identifying the location of the secured service.

1 13. The system of claim 1, wherein the applet provides to the  
2 client a direct connection with the secured service.

1 14. The system of claim 1, further comprising a proxy in  
2 communication with the secured service, and wherein the applet  
3 enables I/O with the proxy.

268040-05674880

1 15. A method comprising the steps of:  
2 establishing a communications link with a client;  
3 determining client privileges;  
4 providing to the client, based on the client privileges, an applet  
5 which enables I/O with a secured service; and  
6 retrieving a key which enables access to the secured service.

1 16. The method of claim 15, wherein establishing a  
2 communications link includes the step of using SSL technology to  
3 create a secure communications link with the client.

1 17. The method of claim 15, wherein establishing a  
2 communications link includes the step of negotiating an encryption  
3 protocol for transferring messages to and from the client.

1 18. The method of claim 15, wherein establishing a  
2 communications link includes the step of using public key certificates  
3 for transferring messages to and from the client.

1 19. The method of claim 15, wherein determining client privileges  
2 includes the step of using public key certificates to authenticate the  
3 client.

00001950-040897

1 20. The method of claim 15, wherein determining client privileges  
2 includes the step of examining client identity and the level of  
3 authentication to determine client privileges.

1 21. The method of claim 15, wherein determining client privileges  
2 includes the step of examining a global certificate to authenticate the  
3 client.

1 22. The method of claim 15, wherein determining client privileges  
2 includes the step of using digital signature technology to authenticate  
3 the client.

1 23. The method of claim 15, wherein establishing a  
2 communications link includes forwarding to the client a security  
3 applet for enabling the client to perform a recognized security  
4 protocol.

1 24. The method of claim 15, further comprising the step of using  
2 the key to communicate through a firewall to the secured service.

268070 05671880

1 25. The method of claim 15, wherein the method is performed by a  
2 global server and further comprising using a global firewall to  
3 protect the global server.

1 26. The method of claim 15, further comprising using a service  
2 address to identify the location of the secured service.

1 27. The method of claim 15, wherein providing includes the step of  
2 providing to the client a direct connection with the secured service.

1 28. The method of claim 15, further comprising using a proxy in  
2 communication with the secured service, and wherein providing  
3 includes enabling I/O with the proxy.

1 29. A system comprising:  
2 means for establishing a communications link with a client;  
3 means for determining client privileges;  
4 means for providing to the client, based on the client privileges,  
5 an applet which enables I/O with a secured service; and  
6 means for retrieving a key which enables access to the secured  
7 service.

268040-0567-880

- 1 30. A computer-based storage medium storing a program for  
2 causing a computer to perform the steps of:  
3 establishing a communications link with a client;  
4 determining client privileges;  
5 providing to the client, based on the client privileges, an applet  
6 which enables I/O with a secured service; and  
7 ~~retrieving a key which enables access to the secured service.~~

268040" 056743